05-23-06

AF/ 1744

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No.:	09/843,069	Confirmation No.: 8483
Applicant:	Burnett et al.	
Filed:	April 26, 2001	
TC/A.U.	2132	
Examiner:	Kristin M. Derwich	
Docket No.:	AUS920010161US1	
Customer No.:	46129	
Title:	METHOD FOR ADDING AND ENFORCING ENHANCED AUTHORIZATION POLICY ON DEVICES IN COMPUTER OPERATION SYSTEMS	

Honorable Commissioner
P. O. Box 1450
Alexandria, Virginia 22313-1450

Express Mail" Mailing Label
Number EQ 460669385 US
Date of Deposit May 22, 2006
I hereby certify that this paper or fee is being deposited with the United States Postal Services "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Commissioner of Patents and Trademarks, P. O. Box 1450 Alexandria, Virginia 22313-1450

Darcell Walker, Reg. No. 34,945

FEE TRANSMITTAL OF APPEALLANT'S BRIEF IN RESPONSE TO OFFICE ACTION UNDER

Applicant files the attached Appeal Brief in support of the Notice of Appeal filed by Applicant on March 20, 2006 in the above-identified application. Please charge the fee of $500.00 to Deposit Account No. 09-0447. The due date to file the Appeal Brief in support of appeal was May 20, 2006. Therefore the filing of the brief is considered timely filed.

Respectfully submitted,

Darcell Walker
Reg. No. 34,945
9301 Southwest Freeway, Suite 250
Houston, Texas 77074
713-772-1255
May 22, 2006

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No.:	09/843,069	Confirmation No.: 8483
Applicant:	Burnett et al.	
Filed:	April 26, 2001	
TC/A.U.	2132	
Examiner:	Kristin M. Derwich	
Docket No.:	AUS920010161US1	
Customer No.:	46129	
Title:	METHOD FOR ADDING AND ENFORCING ENHANCED AUTHORIZATION POLICY ON DEVICES IN COMPUTER OPERATION SYSTEMS	

Honorable Commissioner
P. O. Box 1450
Alexandria, Virginia 22313-1450

Express Mail" Mailing Label
Number EQ 460669385 US
Date of Deposit May 22, 2006
I hereby certify that this paper or fee is being deposited with the United States Postal Services "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Commissioner of Patents and Trademarks, P. O. Box 1450 Alexandria, Virginia 22313-1450

Darcell Walker, Reg. No. 34,945

APPEALLANT'S BRIEF IN RESPONSE TO OFFICE ACTION UNDER 37 C.F.R. § 1.192

This brief is filed in triplicate in support of the previously filed Notice of Appeal, which was filed March 20, 2006, which appealed from the decision of the examiner dated October 18, 2005, rejecting claims 1-21. The fee required under 37 C.F.R. § 1.17(c) for filing a brief in support of an appeal is provided in the Transmittal of Appeal Brief filed herewith.

1. REAL PARTY IN INTEREST

The real party in interest in this appeal is International Business Machines Corporation (IBM).

2. RELATED APPEALS AND INTERFERENCES

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such appeals or interferences.

3. STATUS OF CLAIMS

Claims 1-21 are pending in this application; claims 1-21 have been finally rejected; claims 1-21 have been appealed. No claims have been allowed.

4. STATUS OF AMENDMENTS

No current amendments are pending.

5. SUMMARY OF THE CLAIMS

Claim 1 describes a method for controlling access to a computer system device that is being externally accessed through a special device file. This method first retrieves file attributes for a device file resource used in the access attempt. Once the attributes are retrieved, there is a determination of whether the resource that is making the access attempt is a special device file. If the resource making the access attempt is a device file, a search of a mapping database is performed for special device files that represent the system device that is the object of the access attempt. As part of this search, a special device file entry list is generated containing all of the protected device files that represent that system device. Lastly, an authorization decision for the access attempt to the system device is generated. This decision is based on the security policy that governs each device file in the special device file entry list.

Claim 11 describes a method for controlling access to a computing system device being accessed through a device file. The access is controlled through an externally stored resource. This method initially monitors the computing system for activities related to creating and accessing special device files that represent system devices. When there is an attempt to create a special device file, rules defined in the externally stored resource are used as a basis for restricting attempts to create special device files. Lastly, this method restricts special device file accesses based on rules defined in the externally stored resource.

Claim 12 describes a computer program product for controlling access to a computer system device that is being externally accessed through a special device file. This claims is similar to the method described in claim 1. This computer program product comprises instructions for retrieving file attributes for a device file resource used in the access attempt. Once the attributes are retrieved, there are instructions for determining whether the resource that is making the access attempt is a special device file. If the resource making the access attempt is a device file, a search of a mapping database is performed for special device files that represent the system device that is the object of the access attempt. As part of this search, a special device file entry list is generated containing all of the protected device files that represent that system device. Lastly, there are instructions for generating an authorization decision for the access attempt to the system device is generated. This decision is based on the security policy that governs each device file in the special device file entry list.

Claim 20 describes a computer connectable to a distributed computing system that includes special device driver files containing information related to corresponding system devices. This computer system comprises basic components including a processor, operating system and application programs. This system further comprises an externally stored authorization program overlaying the operating system. The externally stored authorization system further augments the standard security controls of the native operating system. A mapping database contained within the external authorization program stores a system device related to protected object name entries for each protected file system object. This computer system further comprises a decision component within the authorization program for controlling access to special device files representing system devices.

6. ARGUMENTS

6.A. – Was 35 U.S.C. § 102(b) properly applied in a rejection of claims 1-21 as being anticipated by Kenton et al. (U.S. Patent 5,479,612)?

Background of the present invention

This invention describes a method for file system security through techniques that control access to the file system resources using externally stored attributes. The invention accomplishes the objective in a file system security by creating an external database containing auxiliary attributes for objects in the file system. This solution incorporates techniques and algorithms for attribute attachment, storage and organization of the associations to these attributes, and subsequent recognition of attached attributes. In this approach, the attributes would define authorization policy for controlling access to objects in the file system. Such a solution would require techniques for associating the defined policy with file system objects, detecting accesses to the objects, locating the appropriate attributes at access time, and then processing the attributes to produce an access decision for granting or denying access to the accessed resource.

Background of Kenton (5,479,612)

Kenton describes a system and method of encouraging computer system customers to purchase licenses before employing certain types of peripheral devices for use with their computer system. The computer system establishes contact with a peripheral device. It then verifies that the peripheral device is supported by the operating system. If the peripheral device is supported, the system determines whether the peripheral device is licensed (and therefore requires a driver license key in order for the peripheral device to be accessed by the system). If the peripheral device requires a driver license, the system determines whether the corresponding driver license key is installed in the keys file of the computer system. If the driver license key is not installed, the system compels (or encourages) installation of the driver license key by (1) displaying a licensing violation message instructing the customer to obtain the proper license; and/or (2) precluding access of the peripheral device by the computer system.

Distinction between Inventions

The both relate to device access and discuss searching a database to find entries related to the device. However, that it were the similarities stop. The methods and goals of the items are very different. The patent deals with a computer device driver allowing the computer as a whole to support access to the device as a whole and it relates to the hardware connection relationship between the computer and the device.

The present invention pertains to methods for advanced fine-grained discretionary access controls on filesystem (objects that represent access paths to devices). Those devices may be physical devices are s/w abstractions of devices. In summary, the present invention is fundamentally about access controls on filesystem objects that represent devices, not access means between the computer and the physical device.

From there, the ensuing claims and descriptions in the Applicants' present invention define different methods, when compared to Kenton, for device access control, and the methods are applied and enforced an access attempts through the filesystem object that represents the device.

Analysis of the Examiner's rejections

The examiner rejects claim 1 as being anticipated by Kenton et al. The examiner asserts that Kenton describes a method for controlling access to a computer system device and that Kenton describes the steps in Applicants' claim 1. First, Kenton does not incorporate the use of device files in its implementation. As stated in Applicants' disclosure, (paragraph [0002], the file is the fundamental object in a computing system for representing system resources. This representation holds true for attached hardware devices and virtual "pseudo" devices that are represented and accessed through a specialized file type known as a "special device file". The device file acts as the portal to the device and its underlying functionality. This type of file contains no data, but has as part of its attributes, information describing the device.

More particularly, claim 1 contains the step: searching a mapping database for special device files that represent the system device that is the object of the access attempt and generating a special device file entry list of all protected device files that represent said system device. The examiner cites Kenton (column 4, lines 29-33; and column 5 lines 18-22). The examiner asserts the Kenton exhibits the functionality of a "mapping database" through the use of device identification information as the look up data base to be compared to a list of devices supported by the operating system.

Applicant asserts that Kenton does not describe this searching step. Kenton does not describe the generating a special device file entry list of all protected device files that represent a system device. Column 4, lines 29-33 of Kenton describe the comparison of device identification information to a list of peripheral devices supported by the operating system. However, Kenton goes on in that same column 4 to describe the list as an internal list. This list is a predetermined static list that is used for each access attempt. This list is not dynamically generated each time there is an access attempt as is the case in the present invention. Referring to Figure 2 step 23, the access decision step uses the entries in the created list to determine whether or not to grant the access request. This step involves a sort comparison of the list entry with security rules. These security rules are more analogous to the internal list described in Kenton. However, this list is in step 23 and not step 19. As mentioned, Kenton does not generate a dynamic list as described in the mapping step (step 19, Figure 2) of the present invention.

The present invention has two comparison type activities. The searching step and the authorization decision step both incorporate a kind of comparison activity. In the searching step, the comparison is part of the mapping and list generating activity. In the decision authorization step, the comparison is also against the security rules. A further note in the decision authorization step is that the decision to allow access is based on an access grant from each special device files in the database that represents the device that is the object of this access attempt. In steps 23-27 each special device file for that object

has to grant access in order for the grant of the access attempt. If one device file does not grant access then the access attempt is denied.

Contrary to the examiner's assertion that all of the elements of claim are disclosed in the cited reference (Kenton 5,479,612), the element of 'searching a mapping database for special device files that represent the system device that is the object of the access attempt and generating a special device file entry list of all protected device files that represent said system device' is not, so the rejection of claim 1 is unsupported by the art and should be withdrawn.

The examiner rejects claim 11 based on Kenton. Claim 11 describes a method for controlling access to a computing system device being accessed through a device file. The examiner asserts that Kenton describes the step of restricting special device file accesses based on rules defined in the externally stored resource. The examiner cites column 5, lines 5 through 8 to support this assertion. Lines 5 through discuss the requiring of a license in order to access a desired peripheral device. This particular step underscores the distinction between Kenton and the present invention. Because the objectives of the inventions are so different, steps that appear to the same or similar are not similar. The present invention contains many more activities than Kenton for Kenton to anticipate the steps in the present invention.

Claim 12 describes a method for controlling access to a computing system device being accessed through a device file. This claim is similar to claim 1 and the arguments for this claim and the claims that depend from it are the same as for claim 1.

Claim 20 describes a computer connectable to a distributed computing system that includes special device driver files containing information related to corresponding system devices. The present claim contains a mapping database within said external authorization program containing a system device to a protected object name entries for each protected file system object. The examiner asserts that Kenton (column 4, lines 29-

33) describe this type of database. First, the database in the present invention is a database contained in an external authorization program. The list in Kenton is an internal list. There is a structural difference between the Kenton list and the mapping database. The fact that the mapping database is externally stored is a key distinction between Kenton and the present invention. The present invention is focus on control using an external and not internal authorization policy. The operations of Kenton appear to be contained within the operating system. In the present invention, the externally stored authorization program overlaying said native operating system. This structural difference necessitates the functional/operational differences between Kenton and the present invention.

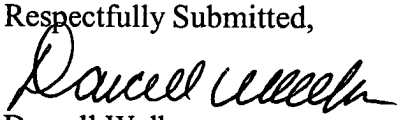
Because of the clear distinctions between in the independent claims between Applicants' invention and the cited reference Kenton, Applicants do not discuss in detail the distinctions in the dependent claims. However, these distinctions further reflect the fundamental differences between Applicants invention and Kenton. One situation that occurs in the present invention that is not in Kenton is when more entries are found during a search. Kenton is basically a one-to-one matching. There is no process where iterative process which requires an acceptance of all entries on the generated list before access is granted. Because the dynamically generated list can have multiple entries, there are steps in the dependent claims that address the iterative process of evaluating each entry on a generated list. There are also steps in the dependent claims that cover the terminating of these iterative processes. These features of the dependent claims further underscore the distinctions between cited reference Kenton and the present invention.

7. CONCLUSION

Applicants submit that all of the pending claims are in condition for allowance. Applicants further submit that the amendments as discussed with the Examiner were for the purpose of further defining the impersonator programs of the present invention. Applicants believe that no additional search should be required in view of the type of amendments Applicants made to the claims. Therefore, withdrawal of the rejections and passage to issuance is respectfully requested.

In view of the above arguments, it is respectfully urged that the rejection of the claims should not be sustained.

Respectfully Submitted,



Darcell Walker
Reg. No. 34,945
9301 Southwest Freeway, Suite 250
Houston, Texas 77074
713-772-1255
May 22, 2006

APPENDIX I CLAIMS

Claim 1 (Previously presented) A method for controlling access to a computer system device, being accessed through a special device file, with externally stored resources comprising the steps of:

retrieving file attributes for a device file resource used in the system device access attempt;

determining whether the resource that is making the access attempt is a special device file;

searching a mapping database for special device files that represent the system device that is the object of the access attempt and generating a special device file entry list of all protected device files that represent said system device; and

generating an authorization decision for the access attempt to the system device based on the security policy that governs each device file in the special device file entry list.

Claim 2 (Original) The method as described in claim 1 further comprising before said searching step the step of terminating said access control method when the accessing resource is not a special device file.

Claim 3 (Previously presented) The method as described in claim 1 further comprising after said searching step the step of terminating said access control method when said searching step did not find any database entries that had device specifications that match device specifications of the special device file making the access attempt.

Claim 4 (Previously presented) The method as described in claim 1 wherein said searching step comprises the steps of: retrieving an entry from the mapping database; comparing device specifications of the special device file making the access attempt to device specifications of the database entry; and comparing the file name of the special device file making the access attempt to the protected object name of the database entry.

Claim 5 (Original) The method as described in claim 4 further comprising after said file name comparison step the steps of: generating a device file entry list containing the database entry with the same file specification and file name as the device file making the access attempt; and terminating said searching step.

Claim 6 (Previously presented) The method as described in claim 4 further comprising after said file name comparison step the steps of placing in a file entry list, a mapping database entry having the same file specification as, but different file name from the special device file making the access attempt.

Claim 7 (Previously presented) The method as described in claim 6 further comprising the steps of:

determining whether there are more entries in the database;

retrieving a next mapping database entry for comparison with said special device file making the access attempt, when more entries are found in the mapping database; and

returning to said special device file comparison step.

Claim 8 (Previously presented) The method as described in claim 2 wherein said authorization decision step comprises the steps of:

retrieving the current entry in the special device file entry list;

calling the access decision component to obtain an access decision for the access attempt to the system device based on the security policy that governs the current entry in the device file entry list;

determining whether decision component granted access;

determining whether more entries are in said special device file entry list, if decision component granted access; and

updating current entry in said special device file entry list and returning to said current entry retrieving step.

Claim 9 (Previously presented) The method as described in claim 8 further comprising after said decision determination step the step of denying the access attempt to the system device if the decision component of a special device file entry denies access.

Claim 10 (Previously presented) The method as described in claim 8 further comprising the step of allowing the access attempt to the system device if no more entries are in the special device file entry list.

Claim 11 (Original) A method for controlling access to a computing system device being accessed through a device file, said access control being through an externally stored resource and comprising the steps of:

monitoring the computing system for activities related to creating and accessing special device files that represent system devices;

restricting the creation of special device files based on rules defined in the externally stored resource; and

restricting special device file accesses based on rules defined in the externally stored resource.

Claim 12 (Previously presented) A computer program product in a computer readable medium for controlling access to a computer system device, being accessed through a special device file, with externally stored resources comprising the steps of:

instructions for retrieving file attributes for a device file resource used in the system device access attempt;

instructions for determining whether the resource that is making the access attempt is a special device file;

instructions for searching a mapping database for special device files that represent the system device that is the object of the access attempt and generating a device file entry list of all protected device files that represent said system device; and

instructions for generating an authorization decision for the access attempt to the system device based on the security policy that governs each device file in the special device file entry list.

Claim 13 (Previously presented) The computer program product as described in claim 12 wherein said instructions for searching a mapping database comprise:

instructions for retrieving an entry from the mapping database;

instructions for comparing the device specification of the special device file making the access attempt to the device specification of the database entry; and

instructions for comparing the file name of the special device file making the access attempt to the protected object name of the database entry.

Claim 14 (Previously presented) The computer program product as described in claim 13 further comprising after said file name comparison instructions: instructions for generating a special device file entry list containing the database entry with the same file specification and file name as the special device file making the access attempt; and instructions for terminating said searching instructions.

Claim 15 (Previously presented) The computer program product as described in claim 13 further comprising after said file name comparison instructions the instructions for placing in a file entry list, a mapping database entry having the same file specification as, but different file name from the special device file making the access attempt.

Claim 16 (Previously presented) The computer program product described in claim 15 further comprising:

instructions for determining whether there are more entries in the database;

instructions for retrieving the next mapping database entry for comparison with said special device file making the access attempt, when more entries are found in the mapping database; and

instructions for returning to said special device file comparison step.

Claim 17 (Presently presented) The computer program product as described in claim 12 wherein said authorization instructions comprise:

instructions for retrieving the current entry in the special device file entry list;

instructions for calling the access decision component to obtain an access decision for the access attempt to the system device based on the security policy that governs the current entry in the device file entry list;

instructions for determining whether decision component granted access;

instructions for determining whether more entries are in said special device file entry list, if decision component granted access; and

instructions for updating current entry in said special device file entry list and returning to said current entry retrieving step.

Claim 18 (Original) The computer program product as described in claim 17 further comprising after said decision determination instructions the instructions for denying the access attempt to the system device if the decision component denies access.

Claim 19 (Previously presented) The computer program product as described in claim 17 further comprising instructions for allowing the access attempt to the system device if no more entries are in the special device file entry list.

Claim 20 (Original) A computer connectable to a distributed computing system, which includes special device files containing information, related to corresponding system devices comprising:

a processor; a native operating system; application programs;

an externally stored authorization program overlaying said native operating system and augmenting the standard security controls of said native operating system;

a mapping database within said external authorization program containing a system device to a protected object name entries for each protected file system object; and

a decision component within said authorization program for controlling access to special device files representing system devices.

Claim 21 (Original) The computer as described in claimed 20 further comprising authorization program for restricting the creation of special device files representing protected system devices.